Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks. Claims 1-21 are pending.

The application is amended to include a reference to the priority claim that was made at filing and indicated on the Filing Receipt. This application was filed August 11, 2000, and the time period for such amendments required of applications filed after November 29, 2000 does not apply.

The Specification is objected to as allegedly including hyperlinks, and the Office action specifically notes that hyperlinks are found on pages 10 and 21. Upon review of the specification, the undersigned is unable to locate any hyperlinks. Clarification is requested.

Claims 1-2, 8-10, and 12-13 are amended to recite a field-representation-select input to clarify that the field-select input previously recited is associated with selection of a particular field type such as a prime field $GF(p)$ or a binary extension field $GF(2^k)$, and not a mere selection of different prime numbers p to select a size of the prime field $GF(p)$. Support for these amendments can be found at, for example, the first paragraph of the Detailed Description at page 6. No new matter is introduced.

Claims 16 and 17 stand rejected under 35 U.S.C. § 101 as allegedly directed to non-statutory subject matter. Claims 16-17 are directed to methods of determining Montgomery products of a first cryptographic parameter and a second cryptographic parameter. Claim 16 is amended to recite combining intermediate values obtained in a series of pipeline stages to obtain a Montgomery product. Various cryptosystems use products such as Montgomery products in, for example, encryption, decryption, authentication, and key distribution. See, for example, Iwamura et al., U.S. Patent 5,321,752 ("Iwamura"), col. 1, line 12 to col. 2, line 43, Monier, U.S.

Patent 5,745,398 ("Monier"), col. 1, lines 12-39. Such methods produce useful and tangible results such as, for example, encrypted, decrypted, or authenticated messages. Therefore, claims 16-17 are directed to statutory subject matter and not mere abstract ideas, and withdrawal of the rejection under 35 U.S.C. § 101 is requested.

Claims 16 and 17 stand rejected under 35 U.S.C. § 112, first paragraph, as one of skill in the art would allegedly not know how to make or use the claimed invention. This rejection is traversed. This rejection is not supported by any specific statements in the Office action concerning such a deficiency. Indeed, Iwamura, Monier, and other prior art cited in the Office action demonstrate that one of skill in the art would know how to make and use an invention concerning methods of implementing Montgomery multiplication in cryptographic systems. Withdrawal of the rejection is requested.

Claims 1, 6, and 12 stand rejected as allegedly anticipated under 35 U.S.C. § 102(e) by CypherCalc: The Cryptographer's Calculator, available from EPS Solutions (referred to as "CypherCalc" herein). This rejection is traversed. First, Applicants note that CypherCalc is not a patent, and therefore cannot serve as a basis for a 35 U.S.C. § 102(e) rejection. Second, the date associated with CypherCalc on PTO Form 892 is March 3, 1999, and apparently results from an Internet search using a date limiter. This date is plainly wrong. The printed materials concerning CypherCalc that accompanied the Office action are noted as "Copyright © 1998-2003," and thus are unlikely to have been available anytime in 1999. See CypherCalc, page 6. The search results noted in the two page Web Search summary include a variety of other obviously incorrect dates. For example, item 3 (dir.jayde.com), item 4 (www.kangarolinks.com), and item 5 (www.wauu) are associated with the date of **December 31, 1969**. These web pages were obviously not available at this date. Moreover, CypherCalc is

noted as being designed for various Windows® operating systems, including Windows XP. CypherCalc at 3. However, Windows XP was apparently not available until 2001, and thus CypherCalc is unlikely to have been available and designed for Windows XP on March 3, 1999, two years before Windows XP was released. (The attached Exhibit contains information concerning the release date of Windows XP.) Finally, the CypherCalc pages cited on form PTO-892 appear to have been downloaded on February 26, 2004. Does the Office contend that these pages precisely describe CypherCalc as it existed on March 3, 1999, almost four years earlier?

In summary, because CypherCalc is not a U.S. patent or patent application publication, withdrawal of the rejection under 35 U.S.C. § 102(e) is requested. In addition, no reliable date can be associated with CypherCalc based on the printed materials provided with the Office action, and CypherCalc cannot be established based on these materials as prior art as of any particular date. Applicants request that a date with some factual support be provided for CypherCalc in any future rejections based on CypherCalc. Accordingly, withdrawal of all rejections based on CypherCalc is requested.

Even if CypherCalc qualified as a proper reference under any section of 35 U.S.C. § 102, CypherCalc does not teach or suggest the combinations of features recited in any pending claim. For example, claim 1 as amended recites a multiplication module that includes

> a first input and a second input configured to receive a first operand and a second operand, respectively, represented as elements of a finite field;
> an output configured to deliver a Montgomery product of the first operand and the second operand; and
> a field- representation-select input configured to select multiplication of the first and second operands based on a selected finite field representation.

While CypherCalc can be used to calculate a Montgomery product of a first and a second operand, CypherCalc requires that field elements be represented as integers modulo a prime number, i.e., as elements of a prime field $GF(p)$, wherein p is a prime number. CypherCalc

apparently permits selection of the prime number p that is stored CypherCalc's "N" operand memory, so that the size of the prime field can be selected. CypherCalc does not teach or suggest representing field elements in any other way such as, for example, as polynomials of length k having coefficients of either 0 or 1, i.e., as elements of the binary extension field $GF(2^k)$. In CypherCalc, operands are represented as integers in hex notation, and CypherCalc is silent concerning any other field representations. Because CypherCalc does not teach or suggest using different field representations, CypherCalc necessarily does not teach or suggest a field-representation-select input as recited in claim 1, and claim 1 and dependent claims 2-5 are properly allowable over CypherCalc.

Claim 6 recites a cryptographic processor that includes a multiplication module configured to receive cryptographic parameters and having processing units configured to determine a Montgomery product of the cryptographic parameters, each processing unit receiving a bit corresponding to the first parameter and partial words of the second parameter. CypherCalc does not teach or suggest such a multiplication module. According to CypherCalc, cryptographic parameters (operands) are entered as complete hex or decimal numbers, and then multiplied. CypherCalc does not teach or suggest processing units that receive a bit from a first parameter and partial words of a second parameter, but instead teaches a single processor that receives all words of all parameters. Therefore, claim 6 and dependent claims 7-12 are properly allowable.

Claim 12 recites a dual-field-representation adder that includes a field-representation-select input and an addition module configured to add values supplied to the first and second inputs according to a value supplied to the field-representation-select input. CypherCalc does not teach or suggest such an adder. CypherCalc is silent concerning representation of operands

in any way other than as integers modulo a prime number, i.e., as elements of a prime field *GF(p)*. Therefore, CypherCalc necessarily fails to teach or suggest a field-representation select input, and claim 12 and dependent claims 13-15 are properly allowable.

Claims 2-4, 8-11,and 19 stand rejected as allegedly obvious from a combination of CypherCalc and Brändström, U.S. Patent 4,322,577 ("Brändström"). This rejection is traversed. Claims 2-4 depend from allowable claim 1, and claims 8-11 depend from allowable claim 6, and these claims are therefore allowable. These claims also recite additional features that are not taught or suggested by these references. For example, claim 3 recites that a first operand is processed bit-wise and a second operand is processed word-wise. The Office action states that CypherCalc's Montgomery Product teaches that a second operand is divided into multiple words that are multiplied with bits of the first operand. CypherCalc merely shows representation of two operands as integers in hex notation and provides no teaching or suggestion of how to multiply the operands such as multiplying words of a first operand by bits of a second operand as recited in claim 3. For at least these reasons, claims 2-4 and 8-11 are properly allowable over CypherCalc and Brändström.

Claim 19 recites a Montgomery multiplier configured to determine a Montgomery product of a first operand and a second operand. The multiplier includes a field-select input for selection of arithmetic operations corresponding to a prime field or a binary extension field, and an output that delivers the Montgomery product. Brändström does not teach or suggest such a Montgomery multiplier. Brändström merely teaches using Galois field arithmetic in a cryptosystem, and Brändström does not teach or suggest a Montgomery multiplier of any kind, particularly a multiplier that includes a field-select input as recited in claim 19. Because no

combination of CypherCalc and Brändström teaches or suggests such a field-select input, claim 19 and dependent claims 20-21 are properly allowable.

Claims 5 and 13-15 stand rejected as allegedly obvious from a combination of CypherCalc and Iwamura et al., U.S. Patent 5,321,752 ("Iwamura"). This rejection is traversed. Iwamura fails to cure the deficiencies of CypherCalc as Iwamura does not teach or suggest multipliers that include a field-representation-select input. These claims depend from allowable claims 1 and 12 and for at least these reasons, claims 5 and 13-15 are properly allowable.

Claims 7 and 16 stand rejected as allegedly obvious from a combination of CypherCalc and Monier, U.S. Patent 5,745,398. This rejection is traversed. Claim 7 is dependent from an allowable base claim and is allowable for at least this reason. Claim 16 recites in part,

> representing the first cryptographic parameter as a series of bits;
> representing the second cryptographic parameter as a series of words;
> determining an intermediate value of a contribution to the Montgomery product based on a first bit of the first cryptographic parameter and the words of the second cryptographic parameter in a first pipeline stage.

Neither CypherCalc nor Monier teaches or suggests such steps. CypherCalc does not teach or suggest determining intermediate values based on a first bit of a first parameter and words of a second parameter. Monier fails to cure the deficiencies of CypherCalc. Monier teaches a multiplication circuit that receives data elements encoded as words. According to Monier, "a multiplication circuit [receives] data elements encoded on at least m' words of k bits [and] encoded words of k bits" Col. 3, lines 46-49. Monier does not teach or suggest determining an intermediate value based on a bit of a first parameter and a word of a second parameter as recited in claim 16. Therefore, claim 16 is properly allowable over any combination of CypherCalc and Monier.

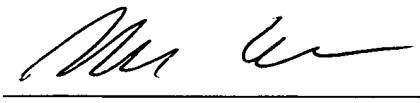
Claims 17-18 stand rejected as allegedly obvious from a combination of CypherCalc, Monier, and Iwamura. Claim 17 recites, in part, a field-select input that selects an addition operation corresponding to addition with carry or without carry. None of the cited references teaches or suggests a field select input or selecting an addition operation based on a selected field such as, for example, a prime field or a binary extension field.

Claims 20-21 stand rejected as allegedly obvious from a combination of CypherCalc, Brändström, and Iwamura. This rejection is traversed. None of these references teaches or suggests a field select input for selecting Montgomery multiplication in different fields such as a prime field and a binary extension field. Therefore, claims 20-21 are properly allowable.

In view of the preceding amendments and remarks, all pending claims are in condition for allowance, and action to such end is requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By 

Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 226-7391
Facsimile: (503) 228-9446

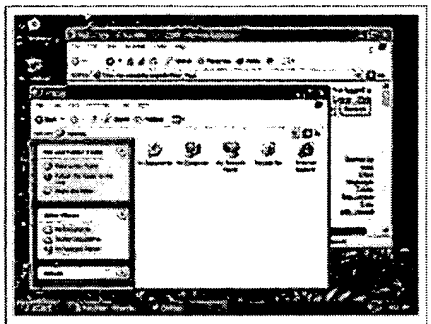
Windows XP

From Wikipedia, the free encyclopedia.

The neutrality of this article is disputed.

The factual accuracy of this article is disputed.

Windows XP (originally code-named *Whistler*) is the latest desktop version of the Windows operating system from the Microsoft Corporation. It was made publicly available on October 25, 2001. Microsoft initially released two editions: **Home** and **Professional**. Home is targeted at home users, while Professional has additional features designed for businesses such as network authentication and dual-processor support. The letters "XP" originate from the word *Experience*.



A typical Windows XP desktop.

Table of contents

Development

Before XP, Microsoft produced two separate lines of operating systems. One line, represented by Windows 95, Windows 98 and Windows Me, was designed for home desktop computers, while the other line, represented by Windows NT and Windows 2000, was aimed at the corporate and professional market, and also included special server versions. Windows XP is Microsoft's attempt to offer a single operating system for all purposes.

Windows XP is based on the Windows 2000 code with a newly developed Graphical User Interface (called Luna), which includes slightly redesigned features. In addition, Windows XP ushered in Microsoft's new "task-based" UI featuring sidebars with access to task-specific functions; marking a shift from the desktop-metaphor used in Mac OS X and most distributions of Linux. However, critics argue that the task-based design only adds visual clutter; as it offers no new functionality over simpler toolbars commonly found in operating systems using the desktop metaphors. Some say that this task-based GUI isn't really that big a change. Others argue that it makes the system more friendly to inexperienced users.

Windows XP home includes a simplified set of the user security features of Windows 2000 and an integrated firewall which was part of a major new effort to secure Microsoft products following a very long history of security issues and vulnerabilities.

Criticisms

EXHIBIT
tabbies